Securing Your Mac & Networks

Security is one of those things that many Mac users don’t like to think about, which is unfortunate, for several reasons. Although Mac OS X enjoys an excellent secure base thanks to its UNIX base, it’s certainly not invulnerable. It behooves Mac users to take all the steps they can to protect their computers and their valuable data. Those family pictures in iPhoto? Your business’ records? Your thesis? The songs you’ve been working on? How would you feel if they disappeared forever? If you don’t protect them, they could. The final reason to learn more about security is my favorite: it’s fun!

Before delving further into tips, advice, and software to enhance your Mac’s security, let me make a recommendation that supersedes everything else: think strongly about paying Undercover to protect your Mac in case of loss or theft. Undercover, available from Orbicule at www.orbicule.com/undercover/, is a virtually undetectable software utility that you install on your Mac. Ideally, you’ll never need to use it, but if your Mac is lost or stolen, you notify Orbicule, and Undercover springs into action, doing the following for you:

- Using Wi-Fi positioning, Undercover finds your Mac within a range of 30-60 feet.
- Displays screenshots that shows what your Mac is doing. If the bad guy e-mails someone, you’ll see it, for instance.
- Takes pictures every eight minutes using your Mac’s iSight camera, giving you a lovely mugshot of your thief.
- Simulate hardware failure, encouraging the perp to sell your Mac or take it into an Apple Store or Apple dealer.
- Once the Mac is in an Apple Store or at an Apple dealer, it will start displaying a message on-screen (and speaking, via your Mac’s built-in text-to-speech) that it has been stolen and will provide Orbicule’s contact info and the promise of a finder’s fee.
This is a sensible series of escalating events that should give you a fighting chance at getting your Mac back. So how much does it cost? $49 for a single Mac, or $59 for a family license that covers five Macs (there are also student and site licenses as well). The family license is a great deal—only $12 per Mac! And there’s no annual fee or anything annoying like that, which is a nice relief.

My good friend Bill Edney had his Mac stolen at a Borders bookstore a year ago. Fortunately, security cameras caught the idiot in the act, so he was busted later. But by that time, Bill’s MacBook Pro was sold and long gone, and he had to buy a new laptop. One of the first things he did with that new laptop? He bought and installed Undercover. Bill’s prepared now; learn from his example and get prepared too.

Managing Passwords

For the foreseeable future, we’re stuck with passwords that we type into little boxes. Sure, there are other options out there—biometrics, two-factor authentication, time-synchronized one-time passwords, public key cryptography, and so on (articles about all of these are on Wikipedia)—but none of them are going to be in wide use for quite some time. As I said, we use passwords now, and we’re stuck with them going forward.

One big problem with passwords, of course, is that most people choose incredibly poor passwords, and then they re-use them on every website and with every login system with which they come into contact. Want to know how bad most passwords are? Check these out:

- “Most Common Hotmail Password Revealed!”
  www.wired.com/threatlevel/2009/10/10000-passwords/

- “Depressing Analysis Of RockYou Hacked Passwords”

- “MySpace password exploit: Crunching the numbers (and letters)”

- “Real-World Passwords”
  hwww.schneier.com/blog/archives/2006/12/realworld_passw.html

Horrible. There are certain rules for creating good passwords—I wrote an article about them called “Pass the Chocolate” for SecurityFocus (www.securityfocus.com/columnists/245)—but the best thing to do is generate long, complicated passwords and then use a password safe like 1Password to store them for you.

I know that some of you are saying, “Why do I need to buy 1Password when Mac OS X comes with Keychain Access in /Applications/Utilities?” Good question. Keychain Access definitely stores passwords in a secure fashion. It’s also free with your OS, which is always nice. But it’s clunky, especially if you want to view your saved passwords: open Keychain Access, click on the site whose password you want to view, check the box next to Show Password, enter your Mac OS X password, and click Allow.